

DESIGNING A MANAGEMENT AND IMPLEMENTATION STRATEGY

After reading this chapter and completing the exercises, you will be able to:

- ◆ Design a strategy for monitoring and managing Windows 2000 network services
- ◆ Use the monitoring and managing tools available to help you get the information you need
- ◆ Develop appropriate response strategies for network problems
- ◆ Design a resource strategy

Hey! We're glad that you made it to this last chapter, which ties together the many pieces of information you learned in this book. This chapter provides you with information on creating a strategy for monitoring and managing Windows 2000 network services. We look at the tools that are available to help you get the information you need and how you can learn to use these tools. We also look at developing a strategy for managing your resources.

STRATEGIES FOR MANAGING AND MONITORING WINDOWS 2000 NETWORK SERVICES

When we speak of strategies here, we really are speaking of how you will spend a finite budget for managing and monitoring network services. With a well-planned strategy, you will find that you can quickly respond to problems and that maintenance will go much more smoothly. Toward that end, we begin this part of the chapter with a discussion on priorities for monitoring Windows 2000 network services. We then examine the tools to be used and determine what needs to be monitored. We end with a detailed discussion of services that play a key role in your success as a network administrator.

Priorities for Monitoring and Managing

When developing a monitoring and management strategy for your network, you will need to decide what needs to be monitored and what has the highest priority. We believe your strategy should have as its first priority maintaining network functionality and availability because your *real* first priority is to ensure that the users of your network can do the work they are employed to do.

To that base goal, you can add this incremental goal: predict and avoid failures before they occur. How do you do this? You determine what is important to measure, and then determine thresholds and limits for those parameters that, once crossed, indicate that action needs to be taken to avoid a network failure. An example of this is setting an alert to warn you when disk space on a server is down to 20% capacity. This warning gives you time to take some action to make more disk space available on the server, before it becomes a crisis.

When the network is functioning solidly, your next incremental goal is to verify compliance with the original design. If you determine that some portion of the network is no longer in compliance with the network design, you will want to evaluate how and why this has happened. It could be that the needs of the organization have changed and that the variation is warning of a change in network usage.

Tools of the Trade

There are many tools available for monitoring network operation. To appreciate the overall health of the network, you will want to use the tools to gather information or troubleshoot on the spot. You also will use tools to automate data and to examine the data you have gathered on a regular basis. The data you collect will reflect the overall performance of the network and monitor the health of specific critical services. In this section, we explore some of the tools you may use for these purposes.

Scripts

Administrators have long relied on scripts to automate repetitive administrative functions. The only native scripting language previously supported by the Windows operating system was the MS-DOS command language. Although fast and small, MS-DOS has limited features when compared to Visual Basic Script and Java Script. Today, ActiveX scripting architecture allows users to take advantage of powerful scripting languages such as Visual Basic Script and Java Script, and MS-DOS command scripts are still supported.

The Windows Scripting Host (WSH) is a language-independent scripting host for 32-bit Windows operating system platforms. Both Visual Basic Script and Java Script scripting engines are included with WSH. ActiveX scripting engines for other languages such as Perl, TCL, REXX, and Python soon will be available from other vendors.

WSH can be run from either the Windows-based host (WSCRIPT.EXE) or the command shell-based host (CSCRIPT.EXE). WSH is integrated into Windows 98, IIS version 4.0, Windows 2000 Server, and Windows 2000 Professional. It also is available for the Windows 95 operating system.

Performance Console

The Performance Console, found in the Start, Programs, Administrative Tools menu, actually has two major parts. First, this is where our old friend Performance Monitor can be found, renamed System Monitor; the second tool is actually a compound tool, Performance Logs and Alerts.

System Monitor is an ActiveX control. ActiveX is a set of technologies that allows software to interact in a networked environment, regardless of the program language of the software. An ActiveX control is a reusable software component that can be used to access ActiveX technology.

System Monitor is the tool to use when you want to immediately see real-time performance, which could be as productive and exciting as watching paint dry. However, this is also the tool you might use to produce reports on monitored data and to view performance logs that you create using Performance Logs and Alerts (see below). System Monitor works with objects, instances of objects, and counters of each object.

When you select an object in System Monitor, data will be gathered on all the counters of the object. However, because the objects often have many counters, System Monitor allows you to select just which counter will be displayed for the Graph, Histogram, or Report views. You can save the data as an HTML file by right-clicking in the details pane and entering a filename. This will be a “frozen” image of the graph, histogram, or report that you may print from your browser. Does this sound too manual for someone with dozens or hundreds of servers to monitor? Read on.

Performance Logs and Alerts is a new service of Windows 2000 that allows administrators to gather data for analysis and to be alerted when predefined events occur or

when thresholds are exceeded. It improves upon and replaces the Performance Data Log of the Windows NT Server 4.0 Resource Kit. This service creates two types of logs—counter and trace—in addition to providing alerts.

You use **counter logs** when you need sampled data from performance objects or counters over time. You use **trace logs** to track performance data associated with events such as disk and file I/O, network I/O, page faults, or thread activity. The event itself triggers the performance data to be sent to the Performance Logs and Alerts service, which will log it. Rather than use the performance counters used by System Monitor and counter logs, trace logs use the Windows 2000 kernel trace data provider. The resulting logs must be viewed using a special parsing tool. The Windows 2000 Server Resource Kit provides two utilities for viewing trace logs: TRACEDMP.EXE and REDUCER.EXE. The Windows NT Server 4.0 Resource Kit also provides a command line tool, TRACELOG.EXE, which can be used to initiate trace logs through scripts.

When using either counter logs or trace logs, you can choose to do sequential logging (for a counter log, you must choose binary to get sequential logging) or circular logging. In sequential logging, as a log file fills up, another log file is created and logging continues. In circular logging, data is recorded continuously to the same log file, overwriting previous data when the file reaches the maximum size. You use sequential logging when disk space is not limited *and* you will monitor disk space to see that you do not run out of disk space. You use circular logging when disk space is an issue *and/or* you do not wish to monitor disk space to ensure that monitoring is not halted by running out of disk space.

In order to be made aware of the occurrence of a specified condition, you can use the Alert function to create an **alert**, define the counters to be used and their thresholds, and define the update interval that you want. You may then define an action to be taken in the event an alert occurs. Actions you can take include run a program, send a message, start a counter log, and update the event log.

Event Viewer Logs

Event Viewer, our old NT 4.0 friend, is also still with us in Windows 2000. With it, we have the basic three event logs—application, system, and security—plus additional logs, depending on the services running on a computer. In addition, on a domain controller, you will also see the Directory Service and File Replication Service logs.

You also can enable enhanced event logging for certain Windows 2000 services, as described in Microsoft Knowledge Base article Q220940, “How to Enable Diagnostic Event Logging for Active Directory Services.” This may be useful for debugging purposes. By default, this logging is set to disable because the amount of data that can be logged can quickly fill the event log.

For years, network administrators have depended on Event Viewer logs to keep them in touch with the health of services. This is where good habits are important. You should develop a schedule for scanning the log files for errors that can indicate a pending failure.

You can calculate uptime based on service stops and starts recorded in the system event logs. Be sure to archive log files both to keep history and as an audit trail, should a problem develop. Reviewing the log files may indicate a problem that you should look for in the future. You can automate the gathering of event log files through the use of scripts.

Last, we urge you to configure the properties of each log file to set the maximum log size and what you want to occur when the maximum size is reached. You also can configure filters to limit the display to the type of events you are searching for, such as failure events.

Simple Network Management Protocol (SNMP) Events

Simple Network Management Protocol (SNMP) is a standard for network management used on both TCP/IP and Internet Package Exchange (IPX) networks. Microsoft supports it by providing an agent that will provide information to SNMP network management systems (NMSs), but they provide no management system (also called a network management console).

The facts around the installation are important to you because when an administrator who does not understand SNMP installs it, a security breach can be created. When the SNMP service is installed, it is far from secure, and it allows any server that uses the default community name of Public read access to SNMP data. In other words, due to the very open default security setting and because this service is run by the system account, anyone can send SNMP instructions to the server and retrieve information or modify the configuration *without* a user name or password! In other words, if you're going to install this service, be sure to change the community strings and restrict access to specific servers!



Your organization may be using an SNMP NMS to manage routers, switches, and hubs, in which case you will want to use that system to manage your Windows 2000 network services. To do this, you must install the SNMP service, which you will do in Hands-on Project 10-1. If you're going to install this service, be sure to change the community strings and coordinate these names with the NMS you are using!

When an NMS server sends a command, or an event occurs for which the SNMP agent was preconfigured, the agent on the device responds to the commands or events by sending status information to the computers hosting the management consoles. The agent provides the information in a standard RFC-specified format, defined as a Management Information Base (MIB). The standardization of this format is useful to you because it opens the doors to the development of tools to retrieve and analyze the data.

The Windows 2000 implementation of SNMP supports several versions of MIB, including the Internet MIB II, LAN Manager MIB II, Host Resources MIB, as well as the Microsoft proprietary MIB. Microsoft does not provide an SNMP console, but many organizations use third-party tools from IBM, Computer Associates, and others to fill the gap.

Microsoft's TCP/IP does include an SNMP agent that will respond to the commands from a third-party management console. In addition, there is a sample graphical SNMP manager program, `SNMPUTILG.EXE` (installed with the Support Tools from the Windows 2000 CD-ROM) that is an example of an application built on top of the Windows 2000 Management Application Programming Interface (API). Once the support tools are installed, `SNMPUTILG.EXE` can be run by selecting Start, Programs, Windows 2000 Support Tools, and Tools.

Network Monitor

Microsoft's Network Monitor allows you to capture and analyze network traffic, looking for the types of traffic generated over selected periods of time. There are two versions of Network Monitor—a “Lite” version and a full version. The “Lite” version comes with Windows 2000 and can only capture traffic sent to or from the computer on which it is running. The full version comes with Microsoft Systems Management Server (SMS) and can put a NIC into promiscuous mode in which all traffic on the network segment can be captured from one computer. If your organization has SMS, this full version is the one you want to use. With this version on a Windows NT or Windows 2000 server, you can monitor all the traffic on a network segment. Additionally, by installing the Network Monitor Driver (also referred to as the agent) on a single Windows NT or Windows 2000 computer, you can gather traffic captured from these other segments using a single server.

Where should Network Monitor fit into your network monitoring and management plan? Well, it is not something you will want to run constantly on your network because if you do, you are adding a processing load to the monitoring machine, and collecting the data adds to network traffic. On the good side, however, Network Monitor allows you to capture data and analyze the traffic. This allows you to define exactly how much traffic is involved in a single user authentication or in the establishment of a connection and a session to a server share. You then can extrapolate the figures to estimate what the network load would be with 500 users or 1000 users authenticating at the same time.

Network Monitor could save your job, or at least help you troubleshoot a problem. An Exchange 2000 consultant related the following eye-opening anecdote to us: He installed and configured the Exchange 2000 Instant Messaging Service at a customer's site. When he tried to log on as an Instant Messaging client, the completed logon box disappeared, and then a blank logon box appeared with no error message on the screen. He then used Network Monitor to capture his next attempt to log on to Instant Messaging. Examining the resulting capture, he saw the subscribe request packets (Instant Messaging logon) from the client to the server, followed by a 404 error in the response packets. This is an HTTP error message that means “not found.” Knowing that when a service cannot be found on a network, the first suspect is name resolution, he then checked the client's DNS settings and the DNS server's records and tracked down

the reason this service could not be found: an incorrect SRV record in DNS. So, although no helpful message displayed on the screen when this logon failed, he was able to troubleshoot it with the help of Network Monitor.

Netdiag

This Windows 2000 command line utility comes with the Windows 2000 Support Tools, on the Windows 2000 CD. Netdiag performs a series of tests on the state of your network client, such as examining .dll files, looking at the output from tests, and checking the system registry. It works with TCP/IP or IPX/SPX.

During execution, Netdiag first checks to see which network protocols or services are running, and then performs some of the more than two dozen tests in its repertoire. To use Netdiag, you must first install the Support Tools. Once they are installed, you can run Netdiag from a command prompt. Run it without any command line parameters to have it perform all the tests appropriate for your network configuration. The results will appear on the screen in the command shell, and will also be written to a file called NETDIAG.LOG saved in the root of the system drive. Output from the Netdiag command will resemble the following:

```

Computer Name: DANVILLE
DNS Host Name: danville.intersales.corp
System info : Windows 2000 Server (Build 2195)
Processor : x86 Family 6 Model 3 Stepping 0,
            AuthenticAMD
List of installed hotfixes :
            Q147222
Netcard queries test . . . . . : Passed
Per interface results:
Adapter : Local Area Connection
Netcard queries test . . . : Passed
Host Name. . . . . : danville
IP Address . . . . . : 192.168.1.203
Subnet Mask. . . . . : 255.255.255.0
Default Gateway. . . . . : 192.168.1.200
Primary WINS Server. . . . : 192.168.1.200
Dns Servers. . . . . : 192.168.2.203
                      192.168.1.200
AutoConfiguration results. . . . . : Passed
Default gateway test . . . : Passed
NetBT name test. . . . . : Passed
    No remote names have been found.
WINS service test. . . . . : Passed
Global results:
Domain membership test . . . . . : Passed
NetBT transports test. . . . . : Passed
List of NetBt transports currently configured:
    NetBT_Tcpip_{65B07788-B626-4F37-9FBB-8EE43FA2A708}

```

```

1 NetBt transport currently configured.
Autonet address test . . . . . : Passed
IP loopback ping test. . . . . : Passed
Default gateway test . . . . . : Passed
NetBT name test. . . . . : Passed
Winsock test . . . . . : Passed
DNS test . . . . . : Passed
Redir and Browser test . . . . . : Passed
    List of NetBt transports currently bound to the Redir
NetBT_Tcpip_{65B07788-B626-4F37-9FBB-8EE43FA2A708}
    The redir is bound to 1 NetBt transport.
    List of NetBt transports currently bound to the browser
NetBT_Tcpip_{65B07788-B626-4F37-9FBB-8EE43FA2A708}
    The browser is bound to 1 NetBt transports.
DC discovery test. . . . . : Passed
DC list test . . . . . : Passed
Trust relationship test. . . . . : Skipped
Kerberos test. . . . . : Passed
LDAP test. . . . . : Passed
Bindings test. . . . . : Passed
WAN configuration test . . . . . : Skipped
    No active remote access connections.
Modem diagnostics test . . . . . : Passed
IP Security test . . . . . : Passed
    IPsec policy service is active, but no policy is
    assigned.
The command completed successfully.

```

In this output, the Netdiag command first lists the computer's name and DNS host name, the operating system and version, the processor type, and the hotfixes installed (listed by Microsoft Knowledge Base article number). The one that appears here, Q147222, may appear although you did not apply this hotfix. We have found this on Windows NT 4.0 after Service Pack 4, and on all the Windows 2000 computers we have tested with Netdiag. This basic information alone is valuable to the administrator who needs to know the service pack and hotfixes installed on a server.

Beyond this initial system information, you will find the results of many network-related tests, discover configuration information about the network interface(s), and test the DNS server, network redirector, and browser. It gives you the status of each of these services from the perspective of the tested machine. If it detects a problem—say, with the DNS name resolution—you can check the listing for the correct DNS server address. If this is correct, you can move on to troubleshoot the network between that computer and the DNS server, and then check the DNS server, if necessary. Netdiag can save you the trouble of running several utilities such as Ipconfig, Nbtstat, and Netstat, to accomplish the same result.

You can find more information about Netdiag in Chapter 3 of the *Windows 2000 Server TCP/IP Core Networking Guide*, which is a book in the Windows 2000 Server Resource Kit from Microsoft. You also can point your Web browser to www.microsoft.com/technet and search for “Netdiag.”

Ping

The Ping command allows you to verify that TCP/IP is configured correctly and allows you to check that you have connectivity to another system. The Ping command sends ICMP Echo Requests, which are returned by the target host. If you receive reply packets when you run the Ping command, it confirms that there is a route between the local computer and the network host you have “pinged.” The Ping command also can be used as a simple test for network latency.

Tracert

Tracert is another vintage TCP/IP command line utility. When you run Tracert, giving it the name of a remote host, it will send packets to that host, revealing the intervening routers. Although Pathping has upstaged it in Windows 2000, Tracert still is a quick way to look at the route to a host, and you are pretty much guaranteed to find it on any vintage Microsoft computer running TCP/IP.

Pathping

Pathping is a command line tool provided with the Windows 2000 TCP/IP stack. It detects packet loss over multiple-hop trips. It combines Ping and Tracert capabilities, while providing more information than either command. You can run the Pathping utility when you are unable to reach a remote host. The Pathping command will report the degree of packet loss at each router along the way, allowing you to determine which routers or links are not functioning properly.

Pathping does its magic by first performing a Tracert, which you see in the first portion of the output. It then displays a computing statistics message while it pings each router in turn to discover where the problem exists. It can take several minutes to perform the pings and the analysis of the data, especially if there are many hops in the route—enough time to grab a cup of coffee or to re-ice your Mountain Dew.

The following code resembles the output received from running the Pathping command to check out the connection to the Course Technology site at www.course.com. The output is normally very verbose, as Pathping performs a DNS name resolution on each router. Our example output is simplified because we used the `-n` command to avoid this name resolution. The actual command line was `pathping -n course.com`.

```
Tracing route to course.com [199.95.72.8] over a maximum of
30 hops:
0 206.145.52.229
1 206.145.48.253
2 206.145.48.254
```

```

3 137.192.160.77
4 137.192.6.241
5 137.192.5.2
6 4.24.149.97
7 4.24.5.241
8 4.24.5.233
9 4.24.9.69
10 4.24.6.22
11 4.24.6.86
12 4.0.5.158
13 4.0.5.230
14 128.11.194.67
15 199.95.72.8 Computing statistics for 375 seconds...
    Source to Here This Node/Link

```

Hop	RTT	Lost/Sent=Pct	Lost/Sent=Pct	Address
0				206.145.52.229
			0/100=0%	
1	117ms	0/100=0%	0/100=0%	206.145.48.253
			0/100=0%	
2	138ms	0/100=0%	0/100=0%	206.145.48.254
			0/100=0%	
3	159ms	18/100=18%	18/100=18%	137.192.160.77
			0/100=0%	
4	152ms	16/100=16%	16/100=16%	137.192.6.241
			0/100=0%	
5	406ms	0/100=0%	0/100=0%	137.192.5.2
			0/100=0%	
6	414ms	1/100=1%	1/100=1%	4.24.149.97
			0/100=0%	
7	414ms	1/100=1%	1/100=1%	4.24.5.241
			0/100=0%	
8	420ms	0/100=0%	0/100=0%	4.24.5.233
			0/100=0%	
9	424ms	0/100=0%	0/100=0%	4.24.9.69
			0/100=0%	
10	415ms	0/100=0%	0/100=0%	4.24.6.22
			0/100=0%	
11	434ms	1/100=1%	1/100=1%	4.24.6.86
			0/100=0%	
12	431ms	0/100=0%	0/100=0%	4.0.5.158
			0/100=0%	
13	426ms	0/100=0%	0/100=0%	4.0.5.230
			0/100=0%	
14	448ms	0/100=0%	0/100=0%	128.11.194.67
			0/100=0%	
15	443ms	0/100=0%	0/100=0%	199.95.72.8

Trace complete.



In the first line of the output, notice that the name *course.com* was resolved to 199.95.72.8. In the first portion of the output, you see the results of a simple route trace to this address, starting at the Internet address of the source of the query, which is on line 0. You can see that the packets traversed 14 routers before arriving at *course.com*. In the second portion of the output, you see the result of Pathping pinging each router, which recorded the packet loss and the round-trip time in milliseconds. This trace completed successfully, but you can see that there was as much as 18% packet loss at certain routers. If *course.com* could not be reached because of a problem at a router, in this last portion, Pathping would indicate which router.

Nslookup

Nslookup is a classic TCP/IP command that allows you to display information queried from DNS name servers. It is a key tool when troubleshooting DNS name resolution problems. Problems can be DNS servers not responding to clients, DNS servers not resolving names correctly, or other general name resolution problems. Using Nslookup, you can query the DNS server to see if it responds and if the responses are valid. This command has two modes: noninteractive and interactive.

If you are just doing a quick test, use noninteractive mode. To run in noninteractive mode, you provide parameters with the Nslookup command. In Figure 10-1, the following command was run: `nslookup carmel liverpool`, where *carmel* was the name of the server to find and *liverpool* was the name of the DNS name server we wanted to query. If you do not provide the name of a DNS server as the second parameter, it will use the default DNS server. The result is the DNS information the DNS server can find about that computer. This information is found in a zone, for which the DNS server is authoritative, or through queries of other DNS servers.

10

```
Command Prompt
C:\>nslookup carmel liverpool
Server:  liverpool.intersales.corp
Address:  192.168.1.200

Name:    carmel.intersales.corp
Address:  192.168.1.204
```

Figure 10-1 Using Nslookup in noninteractive mode on a private network

In Figure 10-2, the computer to find was *www.microsoft.com*, and the DNS name server was not specified, so the default name server was used. In the results, you see the name and IP address of the name server used, as well as the DNS information for *www.microsoft.com*. Notice that this name is actually aliased to several computers. Also, the answer is non-authoritative, because it was not in a zone for which the default name server is authoritative, but it was able to resolve the name through forward lookups.

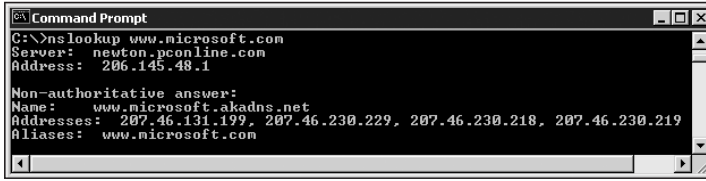


Figure 10-2 Using Nslookup in noninteractive mode on the Internet

If you are troubleshooting and need several pieces of information to analyze, use interactive mode. If you expect to run several queries with Nslookup, also use interactive mode. Simply typing Nslookup from a command prompt gives you interactive mode, which is identified by the Nslookup “>” prompt. At the Nslookup prompt, you can enter Nslookup subcommands.

Nslookup has many subcommands. In the example shown in Figure 10-3, we first ran Nslookup without parameters to access interactive mode. Nslookup displayed the name of the name server to be used, and then displayed the Nslookup prompt. We wanted to verify that the service records for domain controllers for the intersales.corp domain had been registered properly in DNS. To do this, we had to first set the query type to service records with the following Nslookup subcommand: set q=srv. Then, and this is the most nonintuitive part, we entered the name of the record for which we were searching, which was _ldap._tcp.dc._msdcs.intersales.corp. This allowed the return of the name of all registered domain controllers in the intersales.corp domain.



If you are searching for domain controllers in another Active Directory domain, simply use the first part of the service record name and substitute the name of the AD domain in question.

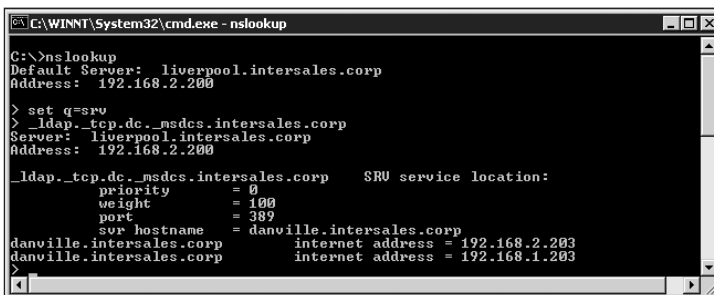


Figure 10-3 Nslookup in interactive mode



For more information on Nslookup, search Windows 2000 Help or enter “help” from Nslookup interactive mode. There is also information in the Windows 2000 Server Resource Kit in the *TCP/IP Core Networking Guide*.

Netstat

The Netstat command is also an old TCP/IP stack favorite, available anytime TCP/IP is installed. It is used to isolate problems to the computer, its connection to the network, or the local network. This command will display protocol statistics and information on current TCP/IP connections.

Netstat has a handful of command line switches: -a, -e, -n, -p, -r, -s, and interval. We illustrate usage of a few of our favorite switches in Figure 10-4. Figure 10-4 first shows the output from running Netstat without a switch, with the -e switch, and finally with the -p switch. The result of running it without a switch was a display of the active connections. The -e switch displays interface statistics. The last example in Figure 10-4 shows the use of the -p switch, which must be followed by the name of a protocol (TCP, UDP, or IP). It shows the connection information for that protocol. Add the -s switch to the last command and it will also display statistics for the protocol, in which case you may use TCP, UDP, IP, or ICMP.

Although not shown in the figure, the -r switch is also useful, as it displays routing info, which can be used to isolate a network problem to routers, especially if you are running RIP or OSPF using Windows 2000 RRAS. The -a switch, another close friend, displays listening ports, which is handy when you're doing security work and you need to see which ports to open on a firewall or if you need to make sure a service is not active.



For more information on Netstat, search the Windows 2000 Help for Netstat, run `netstat /?` from a command prompt to get a summary of available commands, or see the Windows 2000 Server Resource Kit in the *TCP/IP Core Networking Guide*.

```

C:\>netstat
Active Connections
Proto Local Address           Foreign Address         State
TCP    Liverpool:netbios-ssn    carmel.intersales.corp:4247 ESTABLISHED
TCP    Liverpool:3004          danville.intersales.corp:microsoft-ds ESTABLISHED
TCP    Liverpool:3085          danville.intersales.corp:1026 ESTABLISHED

C:\>netstat -e
Interface Statistics
Card Name: Ethernet adapter
Received Sent
Bytes 801660 393209
Unicast packets 3144 2256
Non-unicast packets 1054 91
Discards 0 0
Errors 0 0
Unknown protocols 2559

C:\>netstat -p udp
Active Connections
Proto Local Address           Foreign Address         State

```

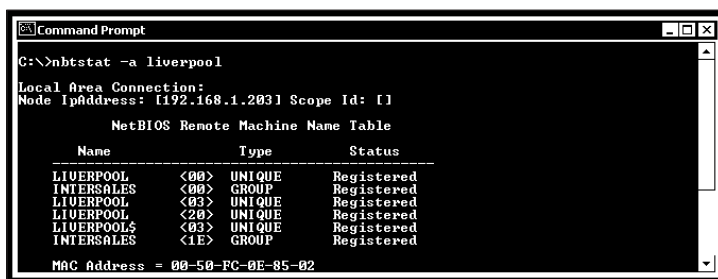
Figure 10-4 Netstat output

Nbtstat

Nbtstat is a command line utility designed to aid in troubleshooting NetBIOS over TCP/IP (NetBT) problems. It comes with the TCP/IP stack on Windows operating systems. Depending on the switches used, it displays the NetBIOS cache on the local or remote computer, purges the name cache and reloads it from an Lmhosts file, does a release/renew of NetBIOS names registered with a WINS server, and lists the current NetBIOS sessions and their status. Although this sounds like a mouthful, it will be very beneficial to you at 3 A.M. when you are trying to figure out why clients are not able to connect to servers.

Experienced network administrators know to check for name resolution problems early in their troubleshooting procedures. Nbtstat is a tool that will allow you to quickly see what address a client computer has resolved from a NetBIOS name. No name resolution or an incorrect address could be a problem with the WINS servers. The next step will be to check the WINS database on the WINS servers for incorrect or outdated information. You are in luck if your WINS servers are running Windows 2000, because of the improvements which will prevent some of the problems we had in the past and allow an administrator to remove incorrect data from the WINS database.

Figure 10-5 shows Nbtstat run with the `-a` switch to query and display the NetBIOS name cache from the remote server, Liverpool. For more information about this command, search the Microsoft TechNet site at www.microsoft.com/technet or check out the *TCP/IP Core Networking Guide* Windows 2000 Server Resource Kit.



```

C:\>nbtstat -a liverpool
Local Area Connection:
Node IpAddress: [192.168.1.203] Scope Id: []

    NetBIOS Remote Machine Name Table

    Name                Type             Status
    ----                -
    LIVERPOOL            <00>             UNIQUE          Registered
    INTERSALES           <00>             GROUP           Registered
    LIVERPOOL            <03>             UNIQUE          Registered
    LIVERPOOL            <20>             UNIQUE          Registered
    LIVERPOOL$           <03>             UNIQUE          Registered
    INTERSALES           <1E>             GROUP           Registered

    MAC Address = 00-50-FC-0E-85-02
  
```

Figure 10-5 Nbtstat sample

Active Directory Administration Tool (Ldp)

The Active Directory Administration Tool is also known as Ldp, which is its filename. Ldp is a GUI tool that can be used to perform LDAP operations on Windows 2000 domain controllers and other LDAP-compatible directories. This feat is important to you because some objects stored in Active Directory do not appear in the standard graphical tools but do appear in Ldp. Therefore, you can use Ldp to view these objects and their metadata.



Metadata is sometimes referred to as “data about data” and can be found in many places. For instance, within a word-processing document, metadata contains information about the author and formatting information for displaying and printing the document. Metadata on a disk volume contains information that enables the file system to store and retrieve files. In Active Directory, metadata is information about the objects and their relationship with other objects and Active Directory. Some examples of Active Directory metadata information are data related to the updating of an object and its attributes and data about the replication relationships between sites. Therefore, metadata is the glue that binds Active Directory together.

You can use Ldp to test connectivity to Global Catalog (GC) servers, as shown in Figure 10-6. On the first line of the detail pane, Ldp attempts to connect to the domain controller Carmel using port 3268. The second line shows that it failed to connect to Carmel. In the third line, a GC connection is attempted to the domain controller Danville. The fourth line shows a successful connection to Danville, followed by lines of retrieved information. In this case, Carmel is not actually a GC server; but if it were, this would indicate a possible failure.

Next you could use Ldp to connect to Carmel using port 389; it should respond as a domain controller. If this succeeds, the last line of the display will indicate whether it is a GC server. If it is, and you cannot connect through port 3268, you need to investigate further because something's afoot. This would require using Network Monitor to capture traffic coming to and from the GC server and using System Monitor to monitor, too.

10

```

ldap://danville.intersales.corp/DC=intersales,DC=corp
Connection Browse View Options Utilities
ld = ldap_open["carmel", 3268];
Error <0x0>: Fail to connect to carmel.
ld = ldap_open["danville", 3268];
Established connection to danville.
Retrieving base DSA information...
Result <0>: (null)
Matched DNs:
Getting 1 entries:
>> Dn:
1> currentTime: 3/23/2001 13:50:53 Central Standard Time Central
Daylight Time;
1> subschemaSubentry:
CN=Aggregate,CN=Schema,CN=Configuration,DC=intersales,DC=corp;
1> dsServiceName: CN=NTDS
Settings,CN=DANVILLE,CN=Servers,CN=Default-First-Site-Name,CN= Sites,CN=Co
nfiguration,DC=intersales,DC=corp;
3> namingContexts:
CN=Schema,CN=Configuration,DC=intersales,DC=corp;
CN=Configuration,DC=intersales,DC=corp; DC=intersales,DC=corp;
1> defaultNamingContext: DC=intersales,DC=corp;
1> schemaNamingContext:

```

Figure 10-6 Using Ldp to test connectivity to Global Catalog servers

Active Directory Services Interfaces Editor (ADSIEdit)

Active Directory Services Interfaces Editor (ADSIEdit) is a Microsoft Management console that can be used as a low-level editor for Active Directory using the Active Directory Services Interfaces. As such, it is more of a management tool than a monitoring tool. You should note that Active Directory Services Interface is an API for Active Directory that enables access to Active Directory by exposing objects stored in the directory as COM objects. You might not think that's a big deal, but it will allow an administrator to add, delete, and move objects within Active Directory. ADSIEdit shines as a search tool for administrators, because a query is created as a container (which can be reused by the administrator or others to whom the administrator delegates tasks).

Replication Monitor (Replmon)

Replication Monitor Replmon is a tool that comes with Support Tools on the Windows 2000 Server CD. Although it runs from an executable REPLMON.EXE, it depends on the presence of several files that are installed when you install Support Tools from the Support\Tools directory. Use Replmon to monitor the replication partners by replication and by partition. Figure 10-7 shows the Replication Monitor console with replication status information.

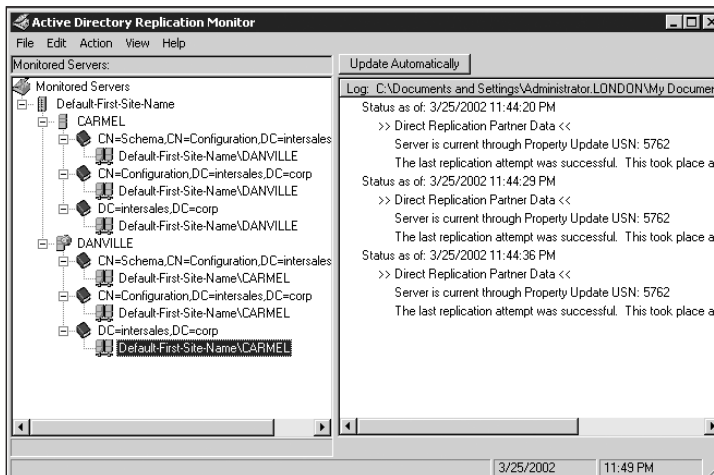


Figure 10-7 Replication Monitor console

Replication Monitor is installed when you install the Support Tools. For more information, see the Tools Help program in the Support Tools menu.

Deciding What and How to Monitor

To effectively monitor network performance without negatively affecting the performance of the network you are trying to manage, you must carefully choose what to monitor to detect service variations. If you simply monitor everything that can be monitored, you will find yourself overwhelmed with data and your monitored systems will be so busy that they won't be able to do the work they were intended to do.

Further exacerbating the "What to monitor?" issue is the fact that responsibilities may be divided in some organizations, with one group responsible for the servers and another group responsible for the network infrastructure. Each group may consider itself the owner of their "turf," but in reality there is considerable overlap. What's the problem with this? Well, the server group may decide that network performance needs to be monitored, but the network group may discount the concerns of the server group for a variety of reasons, especially if the monitoring costs come out of their budget. You need to know in advance that deciding what to monitor is part technical and part personnel. Be prepared.

The various tools we will explore in the coming sections of the chapter will allow you to gather data on the health of your network services. Fair warning—if you are not thoughtful in your planning, you could easily gather more data than could be analyzed in ten lifetimes. One simple technique that will save you from wading through vast amounts of data is to set thresholds for certain critical servers and alerts to notify administrators that the service has exceeded a threshold. This will give people time to react and to solve a pending problem before it becomes a true disaster.

You need a strategy for data collection. If you use **decentralized data collection**, the data is gathered at multiple places out in the network. A large organization with distributed support services would use this strategy. Servers distributed at the sites can gather the data; local staff can be alerted to problems and can react more quickly to solve detected problems. Of course, you can actually combine decentralized and centralized data collection by sending summary information to a central location.

A **centralized data collection** strategy gathers the data at a central point, although it still can be collected from a variety of servers and network devices. You may do this data gathering using in-band data collection or out-of-band data collection.

With **in-band data collection**, the status data traveling to the centralized collection point passes over the same network that is running the services and providing access to users. One problem with in-band data collection is that the flow of the status data itself can affect the results of network measurements. The bigger problem with in-band data occurs if you experience a network failure. Say a WAN link goes down, and your SNMP traps are configured to go across the WAN to your collection station; you won't get the traps because the link is down, so you won't know it's down until your users are complaining. Also, if you need to telnet into a router on the far end to fix it, you won't be able to get there because the WAN link is still down and you'll have to send someone on-site to fix it. The ideal solution is a separate network for management. However, if

your network infrastructure is fault-tolerant or has redundant paths, in-band data collection should have only a minimal effect on the performance measurements and recovery from failures.

If you implement **out-of-band data collection**, the status data travels through a separate network connection from the one that is running the services and providing access to users. This kind of data collection will minimize the impact of the network analysis itself on the network that you are trying to monitor, but it requires another network connection.



We will not attempt to fully educate you in network monitoring, because that takes a great deal of practice and is already well-documented by Microsoft. Your goal with this chapter is only to become proficient in choosing what is important to monitor so that you don't get any nasty surprises when a network service fails. This will allow you to prevent problems or quickly resolve network failures. That way you can be a hero and get your next promotion. For more information (and loads of fun), point your Web browser to www.microsoft.com/technet, click Advanced Search at the top of the screen, enter "network performance" in the search box (without the quotation marks), and select Exact Phrase in the Using box.

An Inventory of Services

You should inventory the services on your network. As part of your network design, you should have this inventory on hand and prioritize it. The services that are most basic to network functionality—name resolution, address allocation, and routing—should be given the highest priority. Without these services, nothing else happens on the network.

In this section we look briefly at each of these services to be monitored. We start by reviewing their function and importance in your network infrastructure and, where appropriate, we list the performance objects that are used for monitoring each of these services.

Lightweight Directory Access Protocol (LDAP) Service

The Lightweight Directory Access Protocol (LDAP) service includes a protocol as well as an associated API. The LDAP API allows programmers to write applications that can use LDAP to query the Active Directory. LDAP is the core protocol for accessing Active Directory over TCP/IP. It is defined as a wire protocol, meaning that LDAP handles the encapsulation and sending of request messages between a client and server. As its name implies, it is small, and it is also fast. LDAP is based on the X.500 standard's Directory Access Protocol.

This is a critical service in an Active Directory domain, because this is the primary protocol Active Directory uses to locate objects. If this protocol does not function, user queries of Active Directory will not occur, and resources located in Active Directory will not be found. Such user queries include transparent queries and explicit queries.

A **transparent query** is one that a user initiates without being aware that they did so. One example of a user action that initiates a transparent query is logon. When a user attempts to log on to a domain, a query is initiated to find a domain controller to service a logon. An **explicit query** is one that the user clearly initiates. An example of an explicit query you may initiate is using the Start Menu Search function to search for printers or for people. Entire Directory will initiate a Global Catalog search, and selecting a domain will initiate a search of that domain. LDAP standard queries begin in the domain where the query started, but can search the entire tree in which the domain resides.

Failed directory searches, coupled with NTDS LDAP Errors in the Directory Service log in Event Viewer, will indicate a problem with LDAP. Your primary tool for directly verifying the health of LDAP is Active Directory Administration Tool (Ldp), a graphical command-line tool that is installed with the Support Tools. The second most important tool for verifying the health of LDAP is Network Monitor, Microsoft's protocol analyzer. Use this tool to capture LDAP traffic. Other tools that can be used to diagnose LDAP problems are Netdiag, Ntdsutil, ADSIEdit, and ADSI Scripts.



Chapter 10 of the *Windows 2000 Server Distributed System Guide*, a book in the Windows 2000 Server Resource Kit, has a detailed sequence of steps to take when diagnosing LDAP problems.

Global Catalog

A Global Catalog (GC) server is a domain controller that stores more information than non-GC domain controllers. All domain controllers store a full copy of the schema and configuration directory partitions, plus a full replica of their own domain directory partition, which means every object and every attribute of every object.

Any domain controller designated to be a GC server holds a partial replica of every object from all the other domains in the forest. Thus, it has every object for the other domains, but only a limited number of attributes for each object for the other domains. The attributes of each object that are replicated to the GC are generally only those objects that are searchable, unique, and accessible. These attributes are defined in the schema as attributes to be replicated to the GC.

What is the value of the GC? It is invaluable for searching and for the logon process. Because the GC contains every object in Active Directory, users and programs can locate objects in the GC by searching on one or more attributes and not need to know in which domain the object exists. GC servers listen on port 3268 while domain controllers listen on port 389.

A GC is searched by default under the following conditions:

- There are applications such as Exchange 2000 that query the GC server. Because these queries are to a port to which only GC servers listen, a non-GC domain controller will not handle them. This will cause the application

to fail to get the response it needs, even though in a single domain AD forest, all domain controllers hold a complete replica of the entire forest. This is especially true of address book lookups, which go to port 3268.

- Any time you select Entire Directory when searching, as when a user initiates a search from the Start menu.
- When a user logs on to a native-mode domain in a multi-domain forest, a GC server must be available (in the same site in which the user's computer resides). If not, the user will not be able to log on unless there are cached credentials on the computer for the user. This is because the logon process needs to check the GC for the user's membership in universal groups. If membership in a universal group is discovered, this is added to the user's logon credentials (access token). The exception to this is Domain Admins, who may log on regardless of the domain mode and the existence of a GC server.
- At logon, if you are using the user principal name rather than a user logon name.

By default, the GC exists on only one domain controller in a forest. Determining the location for GC servers is part of an Active Directory design more than a network design, but you cannot ignore this important function. Simply remember that Microsoft recommends one GC server per Active Directory site, although you may consider having two per site for fault tolerance. If your GC server goes down, users may not be able to log on, and some applications, such as Exchange 2000, which are dependent on accessing the GC may fail to function properly. Remember that Exchange 2000 is heavily dependent on the GC, because all the address book lookups are sent to the GC, not the local domain controller. It's best to have two GC servers on each Windows 2000 site that will host either mail-enabled objects or an Exchange 2000 server.

There are no specific GC performance objects to be measured by System Monitor. As part of Active Directory, the GC depends on the overall health of the Active Directory components, which can be measured through the NTDS performance object.

Domain Controllers

The objectives for Microsoft certification exam 70-221 are light on domain controllers and other heavy-duty issues associated with Active Directory, such as replication, because Active Directory design is the subject of another exam, 70-119. However, you must not ignore domain controllers in your design, because if your network includes Active Directory or NT domains, the domain controllers are central to the network access and to many of the applications.

The rule of thumb is to have at least one domain controller per site. Another (older) rule of thumb has been roughly one domain controller per 2000 users, but this depends entirely on the variables of server configuration, number of attributes per user, network usage per user, number of Active Directory-integrated applications, and more.

You also might consider having at least two domain controllers per site for redundancy. There are a variety of tools used to monitor and manage domain controllers and their functions. These tools include Active Directory Replication Monitor, Ldp, and Performance and Alerts. The key performance object to monitor is NTDS because it contains the performance counters that allow an administrator to monitor such important activity as replication, which is monitored through the DRA counters.

Certificate Services

Certificate Services is a set of services that supports the issuing and managing of certificates used in security systems that include public key technology. Windows 2000 Certificate Services is required if you will be using digital certificates for authentication.

If you need to authenticate users who are not contained within a private database, such as Active Directory, Certificate Services is one of your options. A scenario in which Certificate Service might be employed is for authentication to a B2C site. Additionally, if your design includes using IPSec and Certificate Services authentication, you will need to include Certificate Services.

It is an important thing to install Certificate Services, and should be implemented only after careful planning and study. If Certificate Services has been implemented as part of a network design, you will have to include management and monitoring of this service in your network design. Certificate Services' start, stop, and error events will show in the System Log. The Certification Authority console is the main administrative and monitoring tool for Certificate Services. It tests the service and maintains certification information.

DNS

Distributed Name System (DNS) is an Internet standard hierarchical naming system used to locate resources on the Internet and on private intranets. The DNS service maintains lists of DNS domain names mapped to IP addresses organized into contiguous portions of the DNS namespace known as zones. The DNS service also accepts and responds to queries from DNS clients in order to resolve DNS names to IP addresses. DNS is particularly important in a Windows 2000 Active Directory network, because Active Directory uses the DNS naming hierarchy. DNS is used to resolve host names to IP addresses, IP addresses to host names, and services to host names and IP addresses.



Windows 2000 clients always query DNS when trying to locate an Active Directory object, such as a domain controller. This is a critical service and should be monitored.

Problems with DNS are often associated with human errors in configuring the service and creating records. Thus, an early DNS troubleshooting task should be to reverify configuration settings on the DNS server(s) as well as on hosts. Remember to include your DHCP clients, which receive their DNS configuration from the DHCP server. Check

the configuration settings the DHCP server has for client DNS. Human errors in creating records should go away with Dynamic DNS (DDNS), if you have configured DHCP to update DNS records for pre-Windows 2000 DHCP clients, which cannot update their own DNS records.

Beyond “doing the drill” to verify configuration settings, we still rely on the classic DNS utility, Nslookup, a command-line tool for querying name servers. The newer Netdiag utility also performs DNS tests, and DNS now has a separate log file that can be seen in Event Viewer that records events relating to the updating of records, its ability to access Active Directory integrated zones, and the overall health of the service. You can also monitor the health of DNS and configure alerts through the Performance Console.

DHCP

This is a critical service if your network design includes the use of DHCP for assigning IP addresses and IP configuration to client computers. The DHCP service can integrate with the DNS service to provide dynamic updates of DNS records for the DHCP clients. Now you have two critical network services that must be able to communicate with each other.

DHCP server status can be tracked through the System Event log, which records such events as DHCP startup, authorization, shutdown, and database maintenance tasks. Additionally, the DHCP service has a new audit logging capability that can be enabled or disabled through the DHCP console on the General tab of the DHCP server’s properties sheet. This audit log tracks the actual tasks of the DHCP service, such as IP address leasing, renewal, and release. While you can see the current status of the DHCP server and leases in the DHCP console, the log files allow you to keep a daily history of the server authorization and address leasing activity.

The following output resembles a DHCP log file. The handy table at the beginning of the file documents Event IDs. A listing of the events follows this. Notice the lines recording the frequent DHCP service rogue detection, in which the DHCP services verify that it is, indeed, authorized by Active Directory. The last line of this listing shows Event ID 10, indicating that an IP address has been leased to the computer named “audubon” in the intersales.corp domain. It also shows the physical address of the network card on audubon.

Microsoft DHCP Service Activity Log

Event ID	Meaning
00	The log was started.
01	The log was stopped.
02	The log was temporarily paused due to low disk space.
10	A new IP address was leased to a client.
11	A lease was renewed by a client.
12	A lease was released by a client.
13	An IP address was found to be in use on the network.

- 14 A lease request could not be satisfied because the scope's address pool was exhausted.
- 15 A lease was denied.
- 16 A lease was deleted.
- 17 A lease was expired.
- 20 A BOOTP address was leased to a client.
- 21 A dynamic BOOTP address was leased to a client.
- 22 A BOOTP request could not be satisfied because the scope's address pool for BOOTP was exhausted.
- 23 A BOOTP IP address was deleted after checking to see it was not in use.
- 50+ Codes above 50 are used for Rogue Server Detection information.

```
ID Date,Time,Description,IP Address,Host Name,MAC Address
63,04/12/02,00:54:05,Restarting rogue detection,,,
51,04/12/02,00:55:06,Authorization
succeeded,,intersales.corp,
63,04/12/02,02:01:26,Restarting rogue detection,,,
51,04/12/02,02:02:27,Authorization
succeeded,,intersales.corp,
63,04/12/02,03:08:47,Restarting rogue detection,,,
51,04/12/02,03:09:47,Authorization
succeeded,,intersales.corp,
63,04/12/02,04:16:09,Restarting rogue detection,,,
51,04/12/02,04:17:09,Authorization
succeeded,,intersales.corp,
63,04/12/02,05:23:29,Restarting rogue detection,,,
51,04/12/02,05:24:29,Authorization
succeeded,,intersales.corp,
63,04/12/02,06:30:50,Restarting rogue detection,,,
51,04/12/02,06:31:50,Authorization
succeeded,,intersales.corp,
63,04/12/02,07:38:11,Restarting rogue detection,,,
51,04/12/02,07:39:11,Authorization
succeeded,,intersales.corp,
10,04/12/02,08:22:03,Assign,192.168.2.101,audubon.inter
sales.corp,004090800F4C
```

The Windows 2000 Server online help for DHCP has detailed information about audit logging. This vital service can also be tracked through the Performance console, where you can configure logging of the DHCP object, and it sets alerts to be triggered if certain events occur, such as a DHCP service failure, or if preconfigured thresholds are exceeded.

WINS

Microsoft network clients that predate Windows 2000 still depend on NetBIOS to locate network services. They even locate domain controllers as NetBIOS resources (including Active Directory domain controllers). Similarly, many older applications also depend on NetBIOS. It is highly likely that, for the next few years, you will have one or both of these situations existing on your network and will need to provide a NetBIOS name resolution strategy in your network design. If this is the case, and the design includes WINS, configure your pre-Windows 2000 clients and any Windows 2000 clients running older NetBIOS applications to be WINS clients.

Consider WINS to be a critical service, because these clients will not be able to locate domain controllers beyond their network segment without WINS. WINS service status is reported to the system log, where you can track the health of the service itself.

WINS has an advanced logging option that greatly increases the detail of activity shown in the Event Viewer system log. This is turned on through the Advanced tab of the Properties dialog box of the WINS server in the WINS console. Only turn on this level of logging when you are actively troubleshooting a WINS problem, because it requires considerable system resources. You may also use the Performance console to view performance or create a log of counters of the WINS performance object.

Routing and Remote Access Service (RRAS)

Routing and Remote Access is a multifaceted service, and it covers a lot of territory. It may be your Remote Access service, your NAT server, your internal network router, your IP filter, your demand-dial router, and/or your VPN server. If you are using RRAS for some or all of these functions in your network, then Routing and Remote Access is a critical service for those hosts depending on RRAS.

RRAS performance objects include RAS Port and RAS Total. In addition, RRAS events are logged in the System Event log. If the RRAS itself fails, starts, stops, or has any other error condition, it will be recorded in the System Event log.

You can control the level of logging in the Properties dialog box of the server in Routing and Remote Access console on the Event Logging tab sheet. The first four choices—log errors only, log errors and warnings, log the maximum amount of information, and disable event logging—are self-explanatory and control logging to the System Event log. The last choice logs PPP connection information to a separate log file, PPPLOG, which is stored in the *systemroot*\tracing folder on the RRAS server as it captures the control messages sent and received during a PPP connection attempt. A change to this setting requires a restart of RRAS (not to be confused with rebooting the computer), which you can choose to do as you close the Properties dialog box after changing the setting.



Point-to-Point Protocol logging should be enabled only temporarily when you are troubleshooting a remote access connection problem. This level of logging chews up a great deal of system resources.

Proxy Server

If you are using Proxy Server 2.0 in your Internet connection design, and Internet connectivity is required for people to accomplish their work, you should consider this a critical service. Depending on your implementation, it is providing application proxy services to the Internet for your clients as well as Web caching service.

You may have implemented security features in Proxy Server 2.0 or be using Proxy Server 2.0 in combination with routing and firewall functions on your network. So, if this situation is your reality, you need to be careful that you do not have a single point of failure, such as a single proxy server through which users are accessing Internet applications.

If you have taken steps to provide fault tolerance through cache arrays, individual proxy server performance monitoring may not be that critical. You will have to use your own judgment to establish the frequency and level of monitoring you will perform on the proxy servers. However, if you plan to monitor performance counters for Proxy Server 2.0, read Microsoft Knowledge Base document Q245061, “Proxy Server 2.0 Perfinon View Is Not Saved Correctly in Windows 2000.” This article gives a work around to a problem with incompatible file formats for the views. This article is also your source for the objects and counters you should monitor for proxy server performance.

10

Distributed File System (Dfs)

If Distributed file system (Dfs) is part of your network design, you can monitor its health through the system event log by looking for messages for the Dfs service and for the File Replications Service. Of course, this works only if you have domain dfs roots and have created replicas and enabled automatic replication.

The Dfs console tests the health of a Dfs root or link when you choose Check Status from the Action menu. Two command line tools—Dfsutil and Dfscmd—will allow an administrator to script many administrative functions and generate reports on the status of the service and the components. There are no specific performance objects for Dfs.

DEVELOPING APPROPRIATE RESPONSE STRATEGIES TO NETWORK PROBLEMS

We have looked at the need to monitor network performance, the tools used to gather data on the services, and the services that should be monitored. How should you respond

to the information gathered when it reveals network problems? In general, we have two response modes:

- Reactive, in which you are responding to failures as they occur
- Proactive, in which you are responding to indicators of potential problems before they cause failures

We discuss each in turn.

Planning for Reactive Mode

In reactive mode, you are responding to failures after they occur, either through an automated alert that you defined to notify administrators that a service has failed or through calls to the help desk. Your strategy for planning for reactive mode is to prevent being in that mode in the first place, because in a pure reactive mode, you will have downtime.

Planning for Proactive Mode

When you develop a plan to respond to the data gathered, you are being proactive. Your plan will provide warnings that certain thresholds have been reached or exceeded. For a proactive response strategy, continually gather the following status information (that way, you'll see a thump on the head coming before it actually knocks you to your knees):

- Performance data through System Monitor, and Logging and Alerts
- Services analysis through System Monitor, and Logging and Alerts
- Network traffic management through System Monitor, Logging and Alerts, and Network Monitor
- Server and router congestion status
- Service workload simulation through testing with third-party tools
- Capacity planning trends—also using third-party tools
- Service workload simulation
- Service workload generation

PLAN FOR THE PLACEMENT AND MANAGEMENT OF RESOURCES

You should consider the impact that placement of resources will have on the use of bandwidth. Because we want bandwidth to be used for communicating productive data, we want to minimize the bandwidth used for network overhead. If the resources are placed physically close to where they are needed, they will tend to be more responsive to user requests because they will have more bandwidth available to them. However, you must also consider the reality that the needs of the business, or management-imposed

restraints, may dictate that the resources are located somewhere else. In this event, you need to make sure that the placement of the resource is not going to use bandwidth in some other part of the network to satisfy local user requests. What is important is that you manage the resources so that the network is as efficient as possible, even in the face of unfavorable physical placement.

PLAN FOR GROWTH

In any network infrastructure design, it is essential that you plan for the growth of network resources because it is the nature of networks to grow. If you do not allow for growth, you will have to create a major and painful redesign instead of a graceful evolution. Ideally you would design the network infrastructure so that, even in the face of unexpected growth, you can still have a graceful evolution.

PLAN FOR DECENTRALIZED RESOURCES OR CENTRALIZED RESOURCES

With the advent of NT, Microsoft encouraged the positioning of resources close to the point of usage—meaning that, whenever possible, file and print services, for example, should be made available on the same segment as the clients. This suggested that we should have many modest-sized servers distributed over the network, rather than fewer centrally located large servers. Distribute your servers in this manner when you can.

Note, however, that newer network applications are distributed on the network and/or users need to access data anywhere in the network. In this case, centralize what makes sense, and decentralize what should be distributed close to the users. You will still want to have file and print servers (as well as the printers) close to the users who require them. Large applications managing massive amounts of data are centralized from the users' perspective, even when they include distributed components, like servers and data sources.

Remember, too, that the organization's structure and political environment will have an impact. It is common to have centralized services and administration where everything is located in a single location and/or under a single authority. It is also fairly common to have a decentralized model where both services and administration are physically distributed throughout the organization.

Just because services are decentralized doesn't mean that you can't have centralized administration. In fact, this latter choice may be the correct one to optimize bandwidth usage in a centralized management model. The key thing to remember is that any network still should be as efficient as possible while reflecting the management model with which the organization is most comfortable.

CHAPTER SUMMARY

- When developing your monitoring and management strategy for your network, you will need to decide what needs to be monitored and what has the highest priority. Your first priority should be maintaining network functionality and availability because your *real* first priority is to ensure that the users of your network can do the work they are employed to do.
- There are many tools available for monitoring network operation. To appreciate the overall health of the network, you will want to use the tools to gather information or troubleshoot on the spot. You also will use tools to automate data and to examine the data you have gathered on a regular basis. The data you collect will reflect the overall performance of the network and monitor the health of specific critical services.
- To effectively monitor network performance without negatively affecting the performance of the network you are trying to manage, you must carefully choose what to monitor to detect service variations. If you simply monitor everything that can be monitored, you will find yourself overwhelmed with data and your monitored systems so busy that they cannot do the work they were intended to do.
- You should inventory the services on your network. As part of your network design, you should have this inventory on hand and prioritize it. The services that are most basic to network functionality—name resolution, address allocation, and routing—should be given the highest priority.
- How should you respond to the information gathered when it reveals network problems? In general, we have two response modes: reactive and proactive. In reactive mode, you are responding to failures after they occur, either through an automated alert that you defined to notify administrators that a service has failed or by receiving calls to the help desk. When you develop a plan to respond to the data gathered, you are being proactive. Your plan will provide warnings that certain thresholds have been reached or exceeded.
- You should consider the impact that the placement of resources will have on the use of bandwidth. In addition, in any network infrastructure design, it is essential that you plan for growth of network resources because it is the nature of networks to grow. Last, consider having many modest-sized servers distributed over the network, rather than fewer centrally located servers.

KEY TERMS

alert — In order to be made aware of the occurrence of a specified condition, you may create an alert, define the counters to be used and their thresholds, and define the update interval that you want. You may then define an action to be taken in the event an alert occurs.

- centralized data collection** — Data is gathered at a central point, although it still can be collected from a variety of servers and network devices.
- counter logs** — Track performance data when you need sampled data from performance objects or counters over time. The data is sent to the Performance Logs and Alerts service.
- decentralized data collection** — Data is gathered at multiple places distributed throughout the network.
- explicit query** — A query of Active Directory in which you explicitly and knowingly initiate a search.
- in-band data collection** — Status data collected at a decentralized location travels to the centralized collection point over the same network that is running the services and providing access to users. This has a negative impact on the network you are trying to monitor, and can yield inaccurate data.
- out-of-band data collection** — Status data travels through a separate network connection from the one that is running the services and providing access to users. This kind of data collection minimizes the impact of the network analysis itself on the network that you are trying to monitor.
- Performance Logs and Alerts** — A new service of Windows 2000 that allows administrators to gather data for analysis and to be alerted when predefined events occur or when thresholds are exceeded.
- System Monitor** — A tool, found in the Performance console, to use when you want to immediately see real-time performance, produce reports on monitored data, and/or view performance logs that you create using Performance Logs and Alerts. System Monitor works with objects, instances of objects, and counters of each object.
- trace logs** — Track performance data associated with events such as disk and file I/O, network I/O, page faults, or thread activity. The event itself triggers the performance data to be sent to the Performance Logs and Alerts service.
- transparent query** — A search of Active Directory initiated by an action of the user. The user may not be aware that the action, such as domain logon, initiated an Active Directory search.

REVIEW QUESTIONS

1. You are on the IT staff of an auto parts distributor in Birmingham, AL, with warehouse distribution centers in Mobile, AL, and Jackson, MS. Each site has a LAN as well as a fractional T-1 connection to Birmingham. All IT staffers are located in Birmingham. The other locations have employees who do some IT functions with guidance from the IT staff, but are presently doing things that are not in their job descriptions and that are taking them away from their normal work activities. Briefly describe a general monitoring strategy for this scenario.

2. You have been assigned the task of heading the committee to come up with recommended standards for procedures for your IT organization. What two Web sites would you explore for guidelines on designing these standards?
3. What is your top priority in network monitoring and maintenance?
4. What network events will you respond to with the greatest urgency? (Choose all that apply.)
 - a. a user's logon failure
 - b. failure of the DHCP server on the corporate LAN
 - c. any service or network failure
 - d. A disk on a local file and print server has reached 80% of capacity.
5. A strong network design can fulfill a company's needs for the next three years—guaranteed. True or False?
6. Which tool would you use to monitor real-time performance?
7. Which tool would you use to collect data generated on performance counters?
8. Which tool would you use if you wanted to be warned that certain services had exceeded certain performance thresholds or had failed?
9. Which tool would you use to track performance data associated with events such as disk I/O, network I/O, page faults, and thread activity?
10. Which tool allows you to configure settings for certain log files and to view the logged events?
11. The administrator in charge of a third-party SNMP network management system in your company has called you to complain that she is not receiving MIBs from several of the new Windows 2000 servers that your group has installed. What is a possible cause of this problem and what can you do to correct it?
12. Client computers at one site are having problems locating a domain controller for logon. You believe it may be a DNS problem, but other tests you have done show DNS is functioning properly. How can you actually collect and view the traffic that is generated by a client when the user is attempting to log on?
13. There is a new tool in Windows 2000 that runs several network tests. This is the tool you will want to use before using the tool that is the correct answer for question 12. What is that tool?
14. What is the new tool that seems to combine the capabilities of Tracert and Ping?
15. You can use PATHPING.EXE to test which of the following? (Choose all that apply.)
 - a. DNS
 - b. latency
 - c. which router is failing in a route
 - d. WINS

16. An old but still very useful command line tool for testing DNS is _____.
17. Netstat can be used to isolate a network problem to _____. (Choose all that apply.)
 - a. a computer
 - b. a network connection
 - c. routers
 - d. bridges
 - e. a local network
18. Nbtstat is used to check the DNS cache on a local or remote computer. True or False?
19. What GUI tool that comes with Support Tools allows you to do administration of Active Directory?
20. What is the name of the low-level Active Directory editor that comes with Support Tools?
21. You must administer a multiple-site domain site. Which tool will allow you to view the status of replication?
22. What are the general service variations that you need to monitor on your network?
23. What service actually includes a “wire” protocol as well as an API and is the primary method for accessing Active Directory?
24. What domain controller role is critical for logging on in a multiple domain native mode Active Directory forest?
25. What service must be installed and configured in your network for you to be able to use public key technology for authentication?
26. What is the namespace of Active Directory?

HANDS-ON PROJECTS



Project 10-1 Install and Configure the SNMP Service

For this project, you will need a computer that is running Windows 2000 Advanced Server and that has a connection to the classroom network. You will also need the source files for Windows 2000 Advanced Server. Ask your instructor for this location, and write it in the space below. Use this information, if needed, in Step 17:

If your organization is using an SNMP-based Network Management System (NMS), you may want to allow that management console to manage and monitor your Windows 2000 network services. To enable this, you must install the SNMP Service (also referred to as an agent) on the servers to be managed. In this project, you will install the SNMP Service.

If you are logged on to your Windows 2000 server, you may skip to Step 6. If your server is not powered up, power it up now and start with Step 1.

1. Press **Control/Alt/Delete**.
2. In the User name box, type **administrator**.
3. In the Password box, type **password**. (If this does not work, ask your instructor for the correct password.)
4. In the Log on to box, use the selection arrow to select **INTERSALES**. (This will depend on the classroom configuration.)
5. Press **Enter**.
6. When the desktop appears, open a command prompt.
7. At the command prompt, type **net start**.
8. View the result on your screen. Verify that neither the SNMP Service nor the SNMP Trap Service is started.
9. If neither service is listed, do a further test to ensure that SNMP is not installed, but simply stopped.
10. At the command prompt, type **net start SNMP**. If the SNMP service starts, then it has already been installed, and you can skip to Step 21. If it did not start, then you may proceed to install the SNMP service.
11. From the desktop, click the **Start** button, and then select **Settings, Control Panel, Add/Remove Programs**.
12. Click **Add/Remove Windows Components**.
13. Being very careful *not* to click the check box, locate and click the words **Management and Monitoring Tools**, and then click the **Details** button.
14. In the Management and Monitoring Tools page, click to place a check in the box by **Simple Network Management Protocol**.
15. Click the **OK** button.
16. In the Windows Components page, click the **Next** button.
17. The Configuring Components page appears. If it cannot locate the source files, the Insert Disk dialog box will appear. If this appears, enter the location of the source files in the Copy files from box.
18. The Configuring Components page will show the status of the installation. When it completes, the Completing the Windows Components Wizard page will appear.
19. Click the **Finish** button.
20. Close all open windows.
21. From the desktop, open a command prompt.
22. At the command prompt, type **net start**.
23. View the result on your screen. Verify that both the SNMP Service and the SNMP Trap Service are started. Now you will proceed to configure an SNMP trap to generate SNMP information from the Security Event log to be passed to an SNMP NMS.

24. Close the command prompt.
25. From the Start Menu, select **Programs, Administrative Tools, Computer Management**.
26. In the console tree, expand the **Computer Management** and **Services and Applications** nodes and click **Services**.
27. In the details pane, scroll down until SNMP Service is visible, then double-click **SNMP Service**.
28. In the SNMP Service properties dialog, click the **Traps** tab.
29. On the Traps page, under Community name, type **MyClass** (including the caps—the SNMP Service is case sensitive).
30. Click the **Add to list** button.
31. Click the **Add** button and enter the IP address of the instructor's computer.
32. Click the **Add** button in the SNMP Service Configuration box.
33. Click the **Apply** button on the Traps page, and then click the **Security** tab.
34. Verify that the Send authentication trap check box contains a check, click **public** under Community, and click the **Remove** button.
35. Click the **Add** button.
36. In the SNMP Service Configuration box, verify that READ ONLY is listed under Community rights, and enter **MyClass** (match the case) in the Community Name box.
37. Click the **Add** button.
38. On the Security page, click the **Accept SNMP packets from these hosts** option button.
39. Click the **Add** button and enter the IP address of the instructor's computer.
40. Click the **Add** button in the SNMP Service Configuration box.
41. Click the **OK** button in the SNMP Service Properties dialog box. Close the Computer Management node.

In this project, you installed the SNMP service, a task you would perform on a server you wanted to manage and monitor from a third-party SNMP management console. Once installed, you also configured the SNMP Service to send information to the instructor's computer. In reality, you would give the IP address of a server running an SNMP NMS.



Project 10-2 Use the Performance Console to Configure Trace Logs

For this project, you will need a computer that is running Windows 2000 Advanced Server and has a connection to the classroom network. If you are logged on to your

Windows 2000 server, you may skip to Step 6. If your server is not powered up, power it up now and start with Step 1.

1. Press **Control/Alt/Delete**.
2. In the User name box, type **administrator**.
3. In the Password box, type **password**. (If this does not work, ask your instructor for the correct password.)
4. In the Log on to box, use the selection arrow to select **INTERSALES**. (This will depend on the classroom configuration).
5. Press **Enter**.
6. When the desktop appears, click the **Start** button, select **Programs**, **Administrative Tools**, and click **Performance**.
7. In the Tree pane of the Performance console, expand the **Console Root** (if necessary), and then expand **Performance Logs and Alerts**.
8. Right-click **Trace Logs** and click **New Log Settings**.
9. In the Name box of New Log Settings, type **netlog1**, and then click the **OK** button.
10. In the netlog1 properties dialog box, notice the name consists of the name you provided, plus a suffix, as well as the extension “.etl” for “event trace log.”
11. Click the **Events logged by system provider** button and deselect (remove the checks) for all providers except Network TCP/IP.
12. Click the **Log Files** tab. Normally, you would *not* allow the log files to be saved to your system drive, because this would degrade performance. But for this project, specify a different location *only* if you are low on disk space on drive C and/or if your instructor tells you to use a different location.
13. Ensure that End file names with is selected, and then use the scroll button in the box to select **mmddhhmm**. This will now be the suffix for the files created by this trace.
14. In Log file type, select **Sequential Trace File**.
15. In the Log file size section at the bottom of the Log Files tab sheet, ensure that the Limit of option button is selected and click one of the scroll buttons so that the default value is completely highlighted.
16. Type **1** to replace the default value.
17. Click the **Schedule** tab, and click **Yes** to the resultant dialog box, if necessary.
18. In the Start log section at the top of the Schedule tab sheet, ensure that the At option button is selected, and then make the time five minutes greater than the current time. (There is no real reason to go five minutes out; we just want to make sure the time is at least the current time. If you have been in this box several

- minutes, the time in this box will have lagged behind, and the log may not be triggered.)
19. In the Stop log section, click the **After** option button and use the scroll buttons in the first box to select **15**; use the scroll button in the text box next to the Units to select **minutes**.
 20. At the bottom of the Stop log section under When a log file closes, check the **Start a new log file** check box.
 21. Click the **OK** button, and then click **Trace Logs**. The new trace log appears in the details pane, but it will not start until the time you designated. The icon next to “netlog1” will be red until it is started, at which time it will turn green.
 22. While you are waiting, right-click **Performance Logs and Alerts** in the Tree pane and select **Help**.
 23. Click the **Search** tab of the Help window.
 24. In the Type in the word(s) to search for box, type **sequential**, and then click **List Topics**.
 25. Search through the results that appear and define the term “sequential trace log file” in the space below:

 26. Do a similar search for “circular” and define the term “circular trace log file” below:

 27. Check back at the Performance Console to see if netlog1 has started. If the netlog1 trace log has not started, check the properties of the log to guarantee that they match the settings defined in the steps above.
 28. This process will take a while so, if you wish, you may proceed to the next project. If you choose to do so, complete the next project, return to this one, and continue with the next step.
 29. Open a command prompt and change to the c:\perflogs directory.
 30. Do a directory listing of the perflogs directory. You should now see several trace log files. If you had a tool that would let you view these files, you could view them. They usually have a tremendous amount of information in them. If you have access to the Windows 2000 Server Resource Kit, you can install it and view Tools Help to learn how to use the TRACEDMP.EXE, TRACELOG.EXE, and REDUCER.EXE utilities to work with trace logs.
 31. Close all open windows.



Project 10-3 Use the Performance Console to Configure Alerts

For this project, you will need a computer that is running Windows 2000 Advanced Server and that has a connection to the classroom network. If you are logged on to your Windows 2000 server, or you got here from Step 28 of Project 10-2, you may skip to Step 6. If your server is not powered up, power it up now and start with Step 1.

1. Press **Control/Alt/Delete**.
2. In the User name box, type **administrator**.
3. In the Password box, type **password**. (If this does not work, ask your instructor for the correct password.)
4. In the Log on to box, use the selection arrow to select **INTERSALES**. (This will depend on the classroom configuration.)
5. Press **Enter**.
6. When the desktop appears, click the **Start** button, select **Programs**, **Administrative Tools**, and click **Performance**.
7. In the Tree pane of the Performance Console, expand the **Console Root** (if necessary), and then expand **Performance Logs and Alerts**.
8. Right-click **Alerts**, and select **New Alert Settings**.
9. In the settings box, type **DNS Failure**.
10. Click the **OK** button.
11. In the Comment field, type **Alert for failed DNS Service**.
12. Click the **Add** button below the Counters box.
13. In the Select counters from computer box, enter the name of the class lab domain controller preceded by double backslashes. If the class domain controller is Liverpool, you would type `\\liverpool`.
14. In the Performance object box, select **DNS**.
15. Ensure that **Select counters from list** option button is selected, select **Zone Transfer Failure**, click the **Add** button at the top of the Select Counters page, and then click the **Close** button.
16. On the General tab sheet of the properties for DNS failures, locate the box labeled Alert when the value is, and select **Over**.
17. In the Limit box, type **5**.
18. Click the **Action** tab. Ensure that Log an entry in the application event log is selected and check the **Send a network message to** check box.
19. In the box, enter the name you used to log on. (If you followed the instructions above, it is administrator, but you may have used a different account name.)
20. Click the **OK** button.

In this project, you created an alert to notify you if there are more than five failed zone transfer attempts on the DNS server in your network.



Project 10-4 Use Netdiag to Isolate Network Problems

For this project, you will need a computer that is running Windows 2000 Advanced Server and that has a connection to the classroom network. The Netdiag command will only be available if you have installed the Support Tools from the source CD. To verify

that the Support Tools have been installed, look for them on the Start menu, Programs menu. If they are not there, ask your instructor for the source files for the Support Tools, which are in the Support\Tools directory on the Windows 2000 CD. The Support Tools can be installed by double-clicking on the 2000rkst.msi file. Once the tools are installed, Netdiag can be run from a command prompt.

When you are troubleshooting network connection problems, one of the command line utilities you will use is the Netdiag command. In this project, you will use the Netdiag command as you would use it to detect and isolate a network problem. Although it has several command line switches, it is designed to perform tests and produce an informative report without using any of the switches. In this lab, you will run Netdiag with the /v (verbose) switch and look at the help for Netdiag to see what other switches you can use. If you are logged on to your Windows 2000 server, you may skip to Step 6. If your server is not powered up, power it up now and start with Step 1.

1. Press **Control/Alt/Delete**.
2. In the User name box, type **administrator**.
3. In the Password box, type **password**. (If this does not work, ask your instructor for the correct password.)
4. In the Log on to box, use the selection arrow to select **INTERSALES**. (This will depend on the classroom configuration).
5. Press **Enter**.
6. When the desktop appears, click the **Start** button, and then select **Programs, Accessories, Command Prompt**.
7. At the command prompt, type **netdiag /v >testx.txt** and press **Enter**. The /v will cause the output to be verbose, which means there will be a lot of it. The >testx.txt will cause the output to be written to file testx.txt in the root of the drive that command prompt is running in (probably C:). The x is a number you can choose to create different test files. We are having you write the output to a text file because the command prompt window may not hold it all. The next step will allow you to read the output file.
8. At the command prompt, type **notepad testx.txt**.
9. A Notepad window will open and display the contents of testx.txt, which are the results of running several tests. Are there any failures? If so, discuss them with your classmates and instructor and see if you can resolve them. Read through the information shown to get a feel for what Netdiag shows. Search particularly for DC discovery tests.
10. If you are curious about all available Netdiag tests, at the command prompt type **netdiag ?** and press **Enter**. A list of available switch settings will appear.
11. Close all open windows.



Project 10-5 Use Pathping to Detect a Point of Failure in a Route

For this project, you will need a computer that is running Windows 2000 Advanced Server and that has a connection to the Internet or to another routed network. If you have access to the Internet, you can use “course.com” as the target location. If you do not have a connection to the Internet, but are on a routed network, your instructor will give you the DNS name or IP address of a remote server on your network.

When you are troubleshooting network connection problems, one of the command line utilities you will use is the Pathping command. In this project, you will use the Pathping command as you would use it to detect where a failed router or connection may exist between you computer and the target computer. If you are logged on to your Windows 2000 server, you may skip to Step 7. If your server is not powered up, power it up now and start with Step 1:

1. If your server is not powered up, power it up now.
2. Press **Control/Alt/Delete**.
3. In the User name box, type **administrator**.
4. In the Password box, type **password**. (If this does not work, ask your instructor for the correct password.)
5. In the Log on to box, use the selection arrow to select **INTERSALES**. (This will depend on the classroom configuration.)
6. Press **Enter**.
7. When the desktop appears, click the **Start** button, and then select **Programs, Accessories, Command Prompt**.
8. At the command prompt, type **Pathping -n course.com** and press **Enter**. After it performs a route trace, there will be a delay of several minutes while it pings each router and analyzes the results. Five minutes is not unusual, so relax. You will know when it is completed, because there will be many lines of information on your screen.
9. Verify that the command is completed. After the command is completed, inspect the information displayed and answer the following questions.
10. How many hops in total were displayed?

11. How many hops showed no lost packets?

12. How many hops showed lost packets?

13. Of the hops showing lost packets, what was the largest percentage loss shown?

14. Were the packets able to reach the destination of course.com? How can you tell?

15. Now that you have seen the output without name resolution of the routers, try the same command again without the `-n` parameter. Type **pathping course.com**.
16. Look at the DNS names of the routers. You may see some names that you recognize. If so, discuss these with your classmates and instructor.
17. Close all open windows.



Project 10-6 Use Nslookup for DNS Evaluation

For this project, you will need a computer that is running Windows 2000 Advanced Server and that has a connection to the classroom lab network. In this project, the help desk has reported problems with users logging on to the company's Active Directory domain. They are receiving messages that the domain controllers cannot be found. You suspect it is a DNS problem; so you are going to query the DNS server to see if the domain controllers have registered their SRV records. If your server is powered up and you are logged on, you can skip to Step 7.

1. If your server is not powered up, power it up now.
2. Press **Control/Alt/Delete** to display the Security Dialog box titled Log On to Windows.
3. In the User name box, type **administrator**.
4. In the Password box, type **password**. (If this does not work, ask your instructor for the password.)
5. In the Log on to box, use the selection arrow to select **INTERSALES**. (This will depend on the classroom configuration.)
6. Press **Return**.
7. When the desktop appears, click the **Start** button on the taskbar, point to **Programs**, point to **Accessories**, and then click **Command Prompt**.
8. At the command prompt, type **Nslookup** and press **Enter**.
9. At the command prompt, type **set q=srv**.
10. At the command prompt, type **_ldap._tcp.dc._msdcs.intersales.corp.** (include the final period). (*Note:* You might need to replace "intersales.corp" with the domain name used in your classroom.)
11. Press **Enter**.
12. The result will be the IP addresses and names of all the domain controllers that are registered in the domain. At the Nslookup prompt, type **Exit**.
13. Nslookup also can be run in debug mode, in which you see all the details of the query process. To run debug mode at the command prompt, type **nslookup**.
14. At the Nslookup command prompt, type **set debug**.

15. At the command prompt, type **set q=srv**.
16. At the command prompt, type **_ldap._tcp.dc._msdcs.intersales.corp.** (include the final period). (*Note:* You might need to replace “intersales.corp” with the domain name used in your classroom.)
17. Press **Enter**. This is the same query you performed in earlier steps of this project. In the output, you should see the steps taken to perform the queries, the names and IP addresses of all domain controllers in the domain, and the properties of each record. In both queries, the period was added to the end to indicate that this was a complete FQDN. If you omit the period at the end, Nslookup will append the DNS suffix of the computer you are using to the DNS name you are querying. If that fails, then it queries without the suffix.
18. Close all open windows.



Project 10-7 Use the Netstat Command to Examine Network Statistics

For this project, you will need a computer that is running Windows 2000 Advanced Server and that has a connection to the classroom network. In this project, you are receiving reports that traffic to one server is slow. You want a quick test to try to isolate the problem. If your server is powered up and you are logged on, skip to Step 7.

1. If your server is not powered up, power it up now.
2. Press **Control/Alt/Delete** to display the Security Dialog box titled Log On to Windows.
3. In the User name box, type **administrator**.
4. In the Password box, type **password**. (If this does not work, ask your instructor for the password.)
5. In the Log on to box, use the selection arrow to select **INTERSALES**. (This will depend on the classroom configuration.)
6. Press **Return**.
7. When the desktop appears, click the **Start** button on the taskbar, point to **Programs**, point to **Accessories**, and then click **Command Prompt**.
8. At the command prompt, type **netstat -e** and press **Enter**. The **-e** causes the command to display Ethernet Interface Statistics. Here you are watching for the values in the Discards and Errors rows. Both of these values should be zero, or very low. Errors in the Sent column can indicate a problem with the physical connection to the network or the network itself. These problems could just be that they are overloaded and not adequate for the traffic or that they are, in fact, damaged. Errors in the Received column can indicate a problem with the local network or computer. This could also mean that one or both of these is a bottleneck or that there is a physical problem with the network.

9. At the command prompt, type **netstat -a -n** and press **Enter**. The -a causes the command to display all connections and listening ports. The -n causes the command to not convert addresses and port numbers to names. In both the Local Address and Foreign Address columns, you will see IP addresses followed by a colon and another number. This is a port ID.
10. Point your Web browser to www.isi.edu/in-notes/iana/assignments/port-numbers. This tells you what ports have connections and to which ports the server is listening. See how many ports you can identify on the results of the Netstat command.
11. At the command prompt, type **netstat -s** and press **Enter**. The result will be a listing of the statistics by protocol for IP, ICMP, TCP, and UDP. Look for errors and failed connection attempts.
12. Close the command prompt window and log off.

CASE PROJECTS

The RHEX case study is described below. It describes a company and their network infrastructure design, which incorporates design considerations from most of the chapters in this book. All that is missing in this design are the pieces you will fill in when you do the three case projects.

10

RHEX Background

Rex Heavy Equipment eXport (RHEX) is a multinational corporation headquartered in Houston, with large regional offices in Bahrain, Saudi Arabia; Liverpool, United Kingdom; Melbourne, Australia; Mexico City, Mexico; Kuala Lumpur, Malaysia; and Buenos Aires, Argentina. Their market is the oil and gas operations industry worldwide for which they sell, lease, and transport heavy equipment. There are also a number of branch offices reporting to each regional office.

The RHEX Network

RHEX previously had a Windows 2000 NT single master domain model, with the master domain RHEXCorp and the resource domains centered at each of the regional offices with names that matched the city names. The company has just completed a migration to a single Active Directory domain and has converted to native mode. Each city is an Active Directory site. At the same time that they migrated to Windows 2000 Active Directory, they also migrated to Exchange 2000.

All users have Office 2000 and either Windows 98 or Windows 2000 Professional on their desktops and notebook computers. Their order-processing/inventory management system is implemented as a Web application hosted on Windows 2000 Web servers, backed by a SQL database. They use an Internet-based credit verification service. In addition, there are several NetBIOS applications that will be supported on the network for the next year.

All regional sites access the Internet using T-1 connections, where available. In some locations, the link is as slow as 128 Kbps, in which case they have redundant links. All regional sites also have connections to Houston, also based on the optimum bandwidth available at the location. The branches have dedicated links to their respective regional offices. In addition, they use an international Internet provider that has a local presence in each city where RHEX has regional facilities, and mobile users dial up through the Internet and connect to VPN servers in all the locations.

User Distribution

RHEX needs to provide Internet and intranet access to all users of the corporate network to facilitate communications among all the locations. They have users from several departments who travel extensively, and must be able to connect to both the intranet and Internet. Table 10-1 illustrates the distribution of users across all the locations.

Table 10-1 RHEX User Distribution

Location	Senior Management	Sales and Leasing	IT Services	Operations	Totals
Houston	189	96	204	804	1293
Liverpool	6	112	12	913	1043
Bahrain	6	33	11	206	256
Melbourne	6	27	9	196	238
Mexico City	4	26	8	167	205
Kuala Lumpur	6	20	12	125	163
Buenos Aires	4	25	11	153	193
TOTALS	221	339	267	2564	3391

Following is a profile of each type of user and the respective network needs:

- Management includes all top-level management and their executive staff. This includes CEO, CIO, CFO, COO, and the president and vice presidents, as well as the next level, known as directors and the assistants for each of these functions. They require 24/7 access to both their own intranet and the Internet from all locations and also as mobile users. They must always have access to such services as e-mail and use of their application suite and data.
- Sales and Leasing personnel travel 80% of the time and maintain offices in their homes using laptops. They must have access to e-mail, order processing/inventory management, and a credit verification system. These applications comprise the bulk of their usage and work. They run Office 2000 on their laptops, and they are responsible for the data they store locally.

- IT services are centralized in Houston, with a small support staff in each regional office. A few of the corporate IT staff make regular but infrequent trips to the regional offices, at which time they travel with a “pool” laptop and must have Internet access. Staffers in the regional offices are brought into the corporate headquarters quarterly, and each regional IT staff member is brought in twice a year, so that the regional offices always have some IT staff present. The central IT staff must have access to the monitoring and management applications at all locations.
- Operations includes all the staff that support the sales and leasing operations, including shipping, order processing, warehousing, and customer service functions. These users are not mobile, and they need e-mail and intranet access from the desktop. They must have access to the file and print servers at their locations, and most must have access to the order-processing/inventory management system.

Domain Controllers

Microsoft recommends two domain controllers per site for fault tolerance, and has traditionally recommended a rule of thumb of one domain controller per 2000 users per site. After testing and research, the IT staff has concluded that they need more per site, so they have placed four domain controllers in Houston, three in Liverpool, and two in each of the other regional offices.

10

Global Catalog

Global Catalog servers are critical to this design, because they are using Exchange 2000. Therefore, they have assigned the GC role to the domain controller that is the bridge-head server at each site. This will guarantee that the GC gets replicated across the WAN links. The single GC in each site is a Microsoft recommendation. For the sake of redundancy, the IT group has also assigned the GC role to one other DC at each site.

DNS Servers

DNS Servers are critical to the network because Windows 2000 Active Directory now maps to the DNS namespace. The RHEX IT staff design calls for an Active Directory integrated zone; therefore, they have installed the DNS service on two DCs per site.

DHCP Servers

Two DHCP servers are in each of the two largest sites, while one is in each of the other sites. In the larger sites, the staff has implemented DHCP using distributed scopes and placing the DHCP servers on the subnets with the greatest number of users. At each location, the routers support RFC 1542, which is also referred to as BOOTP forwarding. Therefore, the routers on the segments on which the DHCP servers do not reside will be configured to forward DHCP requests.

WINS Servers

WINS servers are part of the design because of the need to support Windows 98 clients and the NetBIOS applications that will be phased out over the next year. The IT staff has decided to run the WINS service on Windows 2000 servers to take advantage of the improvements in WINS. They will have two WINS servers in Houston and two in Liverpool, configured as replication partners. They wanted a less distributed design for WINS because it is a short-term solution. They will split the clients so that roughly half will have the Houston WINS servers as their first and second WINS servers, and the Liverpool servers as their third and fourth WINS servers. The other half of the clients will have this reversed.

Routing and Remote Access (RRAS)

RRAS servers in all locations are providing VPN support for mobile users connecting over the Internet. Houston, Bahrain, and Kuala Lumpur each have an RRAS server configured to accept dial-in access for backup for the dial-in users, who are sometimes in areas where they cannot access the ISP.

Proxy Server

Each location will have proxy server arrays for applications proxy, address hiding, and Web caching. They should benefit from Web caching because they have many users accessing the same sites over and over again.



Case 10-1 A Plan for the Monitoring of Network Resources

Using the RHEX case study, define a monitoring strategy, including the services you would monitor, the priorities you would assign to the services, and the tools you would use for each service. Also describe your strategy for collecting the data resulting from some of the monitoring.



Case 10-2 A Response Strategy to Detected Network Problems

Using the RHEX case study, define a response strategy for resolving the network problems detected through alerts and data gathering. Describe the strategy in terms of both reactive and proactive response modes.



Case 10-3 A Resource Management Strategy

Using the RHEX case study, define a resource strategy in which you plan for the placement and management of resources in terms of centralized and decentralized data collection, and allow for growth in network resources.